

10-05-00

A

**UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)***(Only for new nonprovisional applications under 37 CFR 1.53(b))*Docket No.
DE919990073US1

Total Pages in this Submission

TO THE ASSISTANT COMMISSIONER FOR PATENTSBox Patent Application
Washington, D.C. 20231

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

**SYSTEM AND METHOD FOR DOWNLOADING APPLICATION COMPONENTS
TO A CHIPCARD**

and invented by:

Stefan Hepper, Thomas Schaeck

3511 U.S. PTO
09/679333
10/04/00If a **CONTINUATION APPLICATION**, check appropriate box and supply the requisite information:☒ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Which is a:

☒ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Which is a:

☒ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Enclosed are:

Application Elements

1. ☒ Filing fee as calculated and transmitted as described below
2. ☒ Specification having 26 pages and including the following:
 - a. ☒ Descriptive Title of the Invention
 - b. ☐ Cross References to Related Applications *(if applicable)*
 - c. ☐ Statement Regarding Federally-sponsored Research/Development *(if applicable)*
 - d. ☐ Reference to Microfiche Appendix *(if applicable)*
 - e. ☒ Background of the Invention
 - f. ☒ Brief Summary of the Invention
 - g. ☒ Brief Description of the Drawings *(if drawings filed)*
 - h. ☒ Detailed Description
 - i. ☒ Claim(s) as Classified Below
 - j. ☒ Abstract of the Disclosure

UTILITY PATENT APPLICATION TRANSMITTAL (Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
DE919990073US1

Total Pages in this Submission

Application Elements (Continued)

3. ☒ Drawing(s) (when necessary as prescribed by 35 USC 113)
- a. ☐ Formal Number of Sheets _____
- b. ☒ Informal Number of Sheets Four (4)
4. ☒ Oath or Declaration
- a. ☐ Newly executed (original or copy) ☒ Unexecuted
- b. ☐ Copy from a prior application (37 CFR 1.63(d)) (for continuation/divisional application only)
- c. ☒ With Power of Attorney ☐ Without Power of Attorney
- d. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application,
see 37 C.F.R. 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation By Reference (usable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied
under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby
incorporated by reference therein.
6. ☐ Computer Program in Microfiche (Appendix)
7. ☐ Nucleotide and/or Amino Acid Sequence Submission (if applicable, all must be included)
- a. ☐ Paper Copy
- b. ☐ Computer Readable Copy (identical to computer copy)
- c. ☐ Statement Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

8. ☐ Assignment Papers (cover sheet & document(s))
9. ☐ 37 CFR 3.73(B) Statement (when there is an assignee)
10. ☐ English Translation Document (if applicable)
11. ☐ Information Disclosure Statement/PTO-1449 ☐ Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☒ Acknowledgment postcard
14. ☒ Certificate of Mailing

☐ First Class ☒ Express Mail (Specify Label No.): EL690558879US

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
DE919990073US1

Total Pages in this Submission

Accompanying Application Parts (Continued)

15. ☒ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*

16. ☐ Additional Enclosures *(please identify below):*

--

Request That Application Not Be Published Pursuant To 35 U.S.C. 122(b)(2)

17. ☐ Pursuant to 35 U.S.C. 122(b)(2), Applicant hereby requests that this patent application not be published pursuant to 35 U.S.C. 122(b)(1). Applicant hereby certifies that the invention disclosed in this application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication of applications 18 months after filing of the application.

Warning

An applicant who makes a request not to publish, but who subsequently files in a foreign country or under a multilateral international agreement specified in 35 U.S.C. 122(b)(2)(B)(i), must notify the Director of such filing not later than 45 days after the date of the filing of such foreign or international application. A failure of the applicant to provide such notice within the prescribed period shall result in the application being regarded as abandoned, unless it is shown to the satisfaction of the Director that the delay in submitting the notice was unintentional.

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
DE919990073US1


Total Pages in this Submission

Fee Calculation and Transmittal

CLAIMS AS FILED

For	#Filed	#Allowed	#Extra	Rate	Fee
Total Claims	20	- 20 =	0	x \$18.00	\$0.00
Indep. Claims	4	- 3 =	1	x \$80.00	\$80.00
Multiple Dependent Claims (check if applicable) <input type="checkbox"/>					\$0.00
BASIC FEE					\$710.00
OTHER FEE (specify purpose)					\$0.00
TOTAL FILING FEE					\$790.00

- ☐ A check in the amount of _____ to cover the filing fee is enclosed.
- ☒ The Commissioner is hereby authorized to charge and credit Deposit Account No. 09-0463 (IBM) as described below. A duplicate copy of this sheet is enclosed.
- ☒ Charge the amount of \$790.00 as filing fee.
 - ☒ Credit any overpayment.
 - ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
 - ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).


Signature

Kevin P. Radigan, Esq.
Reg. No. 31,789
HESLIN & ROTHENBERG, P.C.
5 Columbia Circle
Albany, NY 12203
Telephone (518) 452-5600
Facsimile (518) 452-5579

Dated: October 4, 2000

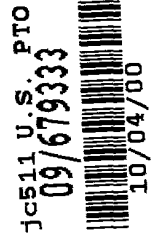
CC:

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

In Re Application of: Hepper et al.

Title: SYSTEM AND METHOD FOR DOWNLOADING APPLICATION
COMPONENTS TO A CHIPCARD

Attorney Docket No.: DE919990073US1 (0560.342)



"EXPRESS MAIL" MAILING LABEL NO. EL690558879US

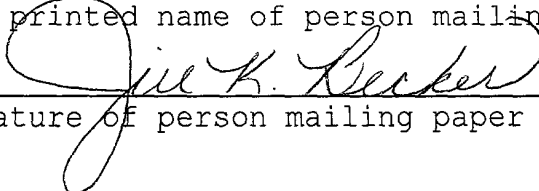
Date of Deposit October 4, 2000

I hereby certify that this paper is being deposited
with the U.S. Postal Service "Express Mail Post Office
to Addressee" service under 37 CFR 1.10 on the date
indicated above and addressed to:

BOX PATENT APPLICATION
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

Jill K. Becker

(Typed or printed name of person mailing paper or fee)


(Signature of person mailing paper or fee)

Enclosures:

- * Utility Patent Application Transmittal Letter (4 pages)
(in duplicate)
- * U.S. Patent Application which includes:
Specification (13 pages), 20 Claims (11 pages),
Abstract (2 pages)
- * Four (4) sheets of Informal Drawings
- * Certified Copy of German Patent Application No. 199 47 986.0
- * Declaration and Power of Attorney for Patent Application
(unexecuted) (3 pages)
- * Two (2) Acknowledgment Postcards

Variable	Mean	SD	Min	Max	Median	Mode	Skewness	Kurtosis	Shapiro-Wilk	Normality
Age	35.2	12.5	18	65	32	30	0.15	2.8	0.98	Normal
Gender	1.2	0.4	1	2	1	1	0.05	1.2	0.99	Normal
Marital Status	2.1	0.8	1	3	2	2	0.10	2.5	0.97	Normal
Education	15.8	2.1	10	20	16	16	0.08	2.9	0.98	Normal
Income	12.5	3.2	5	25	10	10	0.12	3.1	0.96	Normal
Occupation	1.8	0.6	1	3	2	2	0.05	1.5	0.99	Normal
Health Status	2.5	0.7	1	3	2	2	0.08	2.2	0.98	Normal
Stress Level	3.2	1.1	1	5	3	3	0.10	2.8	0.97	Normal
Life Satisfaction	4.1	0.9	3	5	4	4	0.05	1.8	0.99	Normal
Resilience	3.8	1.0	2	5	4	4	0.08	2.5	0.98	Normal
Emotional Stability	4.5	0.8	3	5	4	4	0.05	1.5	0.99	Normal
Physical Health	4.2	0.7	3	5	4	4	0.05	1.5	0.99	Normal
Mental Health	3.9	0.9	3	5	4	4	0.08	2.2	0.98	Normal
Overall Well-being	4.3	0.8	3	5	4	4	0.05	1.5	0.99	Normal

Region	Region	Region
Asia	Asia	Asia
Europe	Europe	Europe
North America	North America	North America
South America	South America	South America
Africa	Africa	Africa
Oceania	Oceania	Oceania
Antarctica	Antarctica	Antarctica
Arctic	Arctic	Arctic
Tropical	Tropical	Tropical
Subtropical	Subtropical	Subtropical
Temperate	Temperate	Temperate
Cold	Cold	Cold
Hot	Hot	Hot
Wet	Wet	Wet
Dry	Dry	Dry
Humid	Humid	Humid
Arid	Arid	Arid
Semi-arid	Semi-arid	Semi-arid
Mountain	Mountain	Mountain
Coastal	Coastal	Coastal
Island	Island	Island
Urban	Urban	Urban
Rural	Rural	Rural
Forest	Forest	Forest
Desert	Desert	Desert
Grassland	Grassland	Grassland
Savanna	Savanna	Savanna
Steppe	Steppe	Steppe
Tundra	Tundra	Tundra
Alpine	Alpine	Alpine
Arctic	Arctic	Arctic
Subarctic	Subarctic	Subarctic
Temperate	Temperate	Temperate
Continental	Continental	Continental
Oceanic	Oceanic	Oceanic
Highland	Highland	Highland
Lowland	Lowland	Lowland
Mountain	Mountain	Mountain
Coastal	Coastal	Coastal
Island	Island	Island
Urban	Urban	Urban
Rural	Rural	Rural
Forest	Forest	Forest
Desert	Desert	Desert
Grassland	Grassland	Grassland
Savanna	Savanna	Savanna
Steppe	Steppe	Steppe
Tundra	Tundra	Tundra
Alpine	Alpine	Alpine
Arctic	Arctic	Arctic
Subarctic	Subarctic	Subarctic
Temperate	Temperate	Temperate
Continental	Continental	Continental
Oceanic	Oceanic	Oceanic
Highland	Highland	Highland
Lowland	Lowland	Lowland
Mountain	Mountain	Mountain
Coastal	Coastal	Coastal
Island	Island	Island
Urban	Urban	Urban
Rural	Rural	Rural
Forest	Forest	Forest
Desert	Desert	Desert
Grassland	Grassland	Grassland
Savanna	Savanna	Savanna
Steppe	Steppe	Steppe
Tundra	Tundra	Tundra
Alpine	Alpine	Alpine
Arctic	Arctic	Arctic
Subarctic	Subarctic	Subarctic
Temperate	Temperate	Temperate
Continental	Continental	Continental
Oceanic	Oceanic	Oceanic
Highland	Highland	Highland
Lowland	Lowland	Lowland
Mountain	Mountain	Mountain
Coastal	Coastal	Coastal
Island	Island	Island
Urban	Urban	Urban
Rural	Rural	Rural
Forest	Forest	Forest
Desert	Desert	Desert
Grassland	Grassland	Grassland
Savanna	Savanna	Savanna
Steppe	Steppe	Steppe
Tundra	Tundra	Tundra
Alpine	Alpine	Alpine
Arctic	Arctic	Arctic
Subarctic	Subarctic	Subarctic
Temperate	Temperate	Temperate
Continental	Continental	Continental
Oceanic	Oceanic	Oceanic
Highland	Highland	Highland
Lowland	Lowland	Lowland
Mountain	Mountain	Mountain
Coastal	Coastal	Coastal
Island	Island	Island
Urban	Urban	Urban
Rural	Rural	Rural
Forest	Forest	Forest
Desert	Desert	Desert
Grassland	Grassland	Grassland
Savanna	Savanna	Savanna
Steppe	Steppe	Steppe
Tundra	Tundra	Tundra
Alpine	Alpine	Alpine
Arctic	Arctic	Arctic
Subarctic	Subarctic	Subarctic
Temperate	Temperate	Temperate
Continental	Continental	Continental
Oceanic	Oceanic	Oceanic
Highland	Highland	Highland
Lowland	Lowland	Lowland
Mountain	Mountain	Mountain
Coastal	Coastal	Coastal
Island	Island	Island
Urban	Urban	Urban
Rural	Rural	Rural
Forest	Forest	Forest
Desert	Desert	Desert
Grassland	Grassland	Grassland
Savanna	Savanna	Savanna
Steppe	Steppe	Steppe
Tundra	Tundra	Tundra
Alpine	Alpine	Alpine
Arctic	Arctic	Arctic
Subarctic	Subarctic	Subarctic
Temperate	Temperate	Temperate
Continental	Continental	Continental
Oceanic	Oceanic	Oceanic
Highland	Highland	Highland
Lowland	Lowland	Lowland
Mountain		

application and the on-card application component, the on-card interface and the security standards. OCF (Open Card Framework) and Microsoft's PC/SC on the other side address the communication between the application, the chipcard reader and the chipcard.

The more widespread use of distributed systems has resulted in an increasing need for downloading of on-card application components to the chipcard via distributed systems. The risks of such methods are obvious. The network is subject to varying loads, so the download may take a long time depending on capacity. Another key aspect in this context is security. All data transfers from the server via the client to the chipcard must be safeguarded. It must be ensured that a simple, secure authentication and encryption method which responds to the varying loads on the network is used when downloading application components.

At present, however, no systems or methods are believed to address this possibility.

Summary of the Invention

It is therefore the object of the present invention to deliver a system and method for downloading application components via distributed systems to a chipcard in a simple manner, taking account of the necessary security checks.

This object is fulfilled by the characteristics of Claims 1, 17, 18 and 20. Advantageous embodiments of the present invention are presented in the sub-claims.

5 The advantages of the present invention lie in the fact that downloading of the application components is divided into two stages.

10 The first stage occurs on the server only, and ensures that not every command to download the application components is sent individually over the network. This is effected by means of an optimized protocol which bundles the individual commands to download the application component into a command sequence and sends it as a data packet over the network. This reduces the time required for downloading application components over the network. Each command within
15 the command sequence is assigned a digital signature and, where appropriate, encrypted. This ensures that only authenticated commands are accepted by the chipcard.

20 In this way this invention meets security requirements for the transfer of data via distributed systems, in particular the Internet.

The second stage occurs between the client and the chipcard, and ensures that the data packets are unpacked and sent individually to the chipcard.

25 All security-relevant keys and certificates are stored on the secure server. Communication between the client and

the server runs preferentially via SSL (Secure Sockets Layer) as the transfer protocol. Misuse of the inventive system/method is thereby rendered much more difficult.

Additional features and advantages are realized through the techniques of the present invention. Other embodiments and aspects of the invention are described in detail herein and are considered a part of the claimed invention.

Brief Description of the Drawings

The subject matter which is regarded as the invention is particularly pointed out and distinctly claimed in the claims at the conclusion of the specification. The foregoing and other objects, features, and advantages of the invention are apparent from the following detailed description taken in conjunction with the accompanying drawings in which:

FIG. 1 shows the state of the art of communication between the off-card application and on-card application component.

FIG. 2 shows a distributed communications architecture on which the present invention is based.

FIG. 3 shows the inventive steps involved in downloading on-card application components from a server over a network to a chipcard.

FIG. 4 shows the inventive architecture in accordance with FIG. 3 in a Java implementation.

FIG. 5 shows the inventive steps involved in downloading on-card application components from a server over a network to a chipcard in a Java implementation.

Best Mode for Carrying Out the Invention

FIG. 1 shows the state of the art in downloading of on-card application components from a terminal to the chipcard and in communication between the on-card application component and off-card application. In the state of the art the chipcard applications consist of an off-card application stored on a terminal and an on-card application component stored on the chipcard in the nonvolatile memory (see FIG.1). The terminal consists of a data processing unit with a chipcard reader and the corresponding driver software for the chipcard reader. The on-card application component communicates with the off-card application over several layers. Layer 1 defines the physical transfer protocol. Layer 2 superimposes that protocol with a logical, byte-oriented protocol. Layer 3 maps higher programming language on layer 2. An example of layer 1 is the protocol T=0, T=1 (ISO/IEC7816-3), layer 2 APDU

protocol (ISO/7816-4), layer 3 OCF (Open Card Framework) or PCSC ().

Normally the on-card application component is transferred to the chipcard via a loader application which runs on the terminal. In this process suitable chipcard commands are used (e.g. for file-oriented chipcards "CREATE" and "UPDATE" commands). At present no solution for the transfer of on-card application components via distributed systems to the chipcard is yet known.

FIG. 2 shows the inventive architecture of the present invention. The inventive architecture is based on a client/server architecture. The client communicates with the server over a network, e.g. the Internet or an Intranet. The client is connected to a chipcard reader and only the server has access to the secret keys required to download on-card application components to the chipcard. The keys may either be stored on the server itself or on another system to which the server has access. The chipcard is protected against unauthorized downloading of on-card application components in such a way that it only accepts commands when they are signed and/or encrypted with the correct keys. On the client a runtime program must exist which communicates both with the chipcard and with the server and which implements a protocol dependent on the respective chipcard.

This protocol specifies when which messages must be exchanged with the chipcard and the server. On the server a runtime program must exist which communicates with the

client and uses the keys accessible to the server as necessary, and which implements a protocol specifying when which messages must be exchanged with the client and when which keys must be used. The chipcards used are common
5 chipcards (such as Java Cards or file-oriented chipcards) which do not have to be adapted for the present invention.

FIG. 3 shows the inventive steps for downloading of on-card application components from a server over a network to a chipcard.

10 The client establishes communication with the chipcard and with the server.

The client sends a request to the server for an on-card application component (application component A) to be placed on the chipcard. The client and server communicate
15 preferentially via TCP/IP or HTTP.

The server sends a response to the client with the request to transmit the chipcard identification data and, where appropriate, a random number for authentication purposes. Chipcard identification data as a minimum contain
20 data relating to the chipcard type and the chipcard number. The client receives the response from the server and sends appropriate command APPUs to the chipcard in order to retrieve the chipcard identification data and, where appropriate, a random number. The chipcard identification
25 data are stored in the nonvolatile memory of the chipcard and can be read by means of suitable commands. The chipcard

receives the commands and returns the chipcard identification data and, where appropriate, the random number to the client. The client sends these data in a request to the server.

5 The server receives the request and evaluates the chipcard identification data to find out which keys have to be used, or to derive the necessary keys from Master Keys, in order to be able to download the application component A. The keys are used to prepare a command sequence for
10 downloading of the application A from the server to the chipcard. This command sequence causes the application A to be created on the chipcard. The command sequence is a predefined sequence stored in the nonvolatile memory area of the server for a specific application. A further embodiment
15 of the invention is that the command sequence is created in whole or in part with the aid of a program on the server. This is preferentially applied where card-specific data are also to be integrated into the on-card application component by means of the command sequence. Preferentially each
20 command within the sequence is signed with the aid of the key (Session Keys) and encrypted as necessary. This can be effected, for example, by assigning the first command within the sequence a MAC (message authentication code) with the aid of the random number and the correct key, and assigning
25 all subsequent commands a MAC based on the MAC of the preceding command and the correct key. The sequence with the signed and, where appropriate, encrypted commands is sent to the client.

The client receives the response with the command sequence and sends the commands consecutively to the chipcard. The chipcard checks the signature and only executes the commands if the signature is correct.

5 FIG. 4 shows the inventive architecture in accordance with FIG. 3 in a Java implementation.

10 On the client a Web Browser is run to enable the user to navigate to the Web page of the server. The Web page of the server contains the applet which implements the client program described in FIG. 3. When the Web page is displayed the applet is downloaded from the server to the Browser. The applet establishes a communication link to a servlet on the server. The servlet has the functionality of the server program.

15 The procedure for downloading the on-card application component corresponds to that set out in FIG. 3.

FIG. 5 shows the inventive steps for downloading of on-card application components from a server over a network to a chipcard in a Java implementation.

20 It is assumed in this that a brokerage application stored on a server is to be loaded into the chipcard. Authentication keys are also stored on the server.

The client establishes communication with the chipcard and with the server. Communication with the chipcard is implemented by OCF (Open Card Framework).

5 The client sends a request to the server for the brokerage application (on-card application component) to be placed on the chipcard. The client and server communicate preferentially via TCP/IP or HTTP.

10 The server sends a response to the client with the request to transmit the chipcard identification data (GetCardInfo).

15 The client receives the response from the server and sends appropriate command APPUs to the chipcard in order to retrieve the chipcard identification data. The chipcard identification data are stored in the nonvolatile memory of the chipcard and can be read by means of suitable commands. The chipcard receives the commands and returns the chipcard identification data to the client. The client sends these data in a request to the server.

20 The server receives the request and evaluates the chipcard identification data to find out the card type. An authentication method is chosen depending on the card type. In the present implementation the card type is a VISA Open Platform card with symmetrical keys. The first authentication step involves the server generating a random
25 number and selecting a key number, and then sending that information packed in a command to the client. The client

extracts the OCF command and sends it to the OCF interface on the client computer. The OCF interface converts the OCF command into one or more APDUs and sends it/them to the chipcard. The chipcard receives the APDUs, identifies them as an authentication command, generates a random number, creates a Session Key from the two random numbers and the transmitted key, and thereby returns the random numbers in encrypted form.

The client transmits the card's response to the server. The server likewise generates a Session Key from the two random numbers and the key number. With the aid of this Session Key it checks the encrypted random numbers. If the check is successful the card is classed as authenticated.

The server sends a second authentication command to the client in order to authenticate itself according to the same method, as already described. If the check is successful the server is classed as authenticated.

The brokerage application is signed on the server by means of the Session Keys and encrypted as necessary in order to be able to download the broker application. This command sequence causes the application A to be created on the chipcard. The command sequence is a predefined sequence stored in the nonvolatile memory area of the server. A further embodiment of the invention is that the command sequence is created in whole or in part with the aid of a program on the server. This is preferentially applied where

card-specific data are also to be integrated into the on-card application component by means of the command sequence.

Preferentially each command within the sequence is signed with the aid of the key (Session Keys) and encrypted as necessary. This can be effected, for example, by assigning the first command within the sequence a MAC (message authentication code) with the aid of the random number and the correct key and assigning all subsequent commands a MAC based on the MAC of the preceding command and the correct key. The sequence with the signed and, where appropriate, encrypted commands is sent to the client.

The client receives the response with the command sequence and sends the commands consecutively to the chipcard. The chipcard checks the signature and only executes the commands if the signature is correct.

The steps outlined can also be used to customize the new application/brokerage application.

The present invention can be included in an article of manufacture (e.g., one or more computer program products) having, for instance, computer usable media. The media has embodied therein, for instance, computer readable program code means for providing and facilitating the capabilities of the present invention. The article of manufacture can be included as a part of a computer system or sold separately.

Additionally, at least one program storage device readable by a machine, tangibly embodying at least one program of instructions executable by the machine to perform the capabilities of the present invention can be provided.

5 The flow diagrams depicted herein are just examples. There may be many variations to these diagrams or the steps (or operations) described therein without departing from the spirit of the invention. For instance, the steps may be performed in a differing order, or steps may be added,
10 deleted or modified. All of these variations are considered a part of the claimed invention.

15 Although preferred embodiments have been depicted and described in detail herein, it will be apparent to those skilled in the relevant art that various modifications, additions, substitutions and the like can be made without departing from the spirit of the invention and these are therefore considered to be within the scope of the invention as defined in the following claims.

Claims

What is claimed is:

1. Method for downloading application components from a server via a client to a chipcard, wherein the server and the client are interconnected via a distributed system, said method comprising:

a) delivery of a secret key or Session Key by the server;

b) loading of a sequence of commands to download the application component to the chipcard;

c) generation of a digital signature with the secret key or Session Key by way of each command within the command sequence;

d) transmission of the signed command sequence as a data packet to the client;

e) unpacking of the data packet and transmission of the individual commands in sequence to the chipcard; and

f) checking of the digital signature of the individual commands and execution of the commands if the digital signature is correct.

2. Method in accordance with Claim 1, wherein the authentication method for generation of the Session Key is selected by:

5 a) transmission of a request from the server via the client to the chipcard to transmit the chipcard identification data stored on the chipcard;

10 b) reading of the chipcard identification data from the nonvolatile memory of the chipcard and transmission of the chipcard identification data via the client to the server; and

15 c) identification from the chipcard identification data of an authentication method by means of which a Session Key agreed between the server and the chipcard can be generated.

3. Method in accordance with Claim 2, wherein the Session Key is determined by an authentication method comprising:

5 a) generation of a random number and selection of a secret key by the server;

b) transmission of the random number in accordance with step a) via the client to the chipcard;

10 c) generation of a random number by the chipcard;

d) creation from the two random numbers and the transmitted keys of a Session Key;

15 e) transmission of the encrypted random numbers and the random number generated by the chipcard to the server; and

f) generation of a Session Key by the server and checking of the encrypted random numbers with the aid of the Session Key.

20 4. Method in accordance with Claim 1, wherein the distributed System is an intranet or an Internet.

5. Method in accordance with Claim 1, wherein communication between the server and the client runs via SSL (Secure Sockets Layer) as the transfer protocol.

6. Method in accordance with Claim 1, wherein on the
5 server a runtime program exists which communicates with the client and uses the keys accessible to the server as necessary, and defines the protocol specifying when which messages must be exchanged with the client and when which keys must be used; and that on the client a runtime program
10 exists which communicates both with the chipcard and with the server and which implements the protocol defining when which messages must be exchanged with the chipcard and the server.

7. Method in accordance with Claim 1, wherein the
15 chipcard identification data as a minimum comprise a chipcard serial number and a chipcard type.

8. Method in accordance with Claim 1, wherein the digital signature is executed by way of a symmetrical cryptoalgorithm with the aid of the Session Key agreed
20 between the client and the server, or by way of an asymmetrical cryptoalgorithm with the aid of a private key located on the chipcard, wherein the server is in possession of the public key.

9. Method in accordance with Claim 8, wherein the symmetrical cryptoalgorithm is DES or Triple-DES and the asymmetrical cryptoalgorithm is RSA, DSA or an Elliptic Curve algorithm.

5 10. Method in accordance with Claim 3, wherein the secret key is derived from the chipcard identification data and the Master Key.

10 11. Method in accordance with Claim 1, wherein the command sequence as a minimum comprises an Install command, one or more Load commands and a final Install command, and is stored in an APDU structure.

12. Method in accordance with Claim 1, wherein each command within the command sequence is encrypted by means of the Session Key.

15 13. Method in accordance with Claim 1, wherein the command sequence is a predefined sequence for a specific application which is stored in the nonvolatile memory of the server and is loaded into volatile memory of the server during the program runtime.

20

14. Method in accordance with Claim 1, wherein the command sequence is generated by the server program, and wherein on the server a runtime program exists which communicates with the client and uses the keys accessible to
5 the server as necessary, and defines the protocol specifying when which messages must be exchanged with the client and when which keys must be used; and that on the client a runtime program exists which communicates both with the chipcard and with the server and which implements the
10 protocol defining when which messages must be exchanged with the chipcard and the server.

15. Method in accordance with Claim 14, wherein card-specific data are integrated into the command sequence.

16. Method in accordance with Claim 13, wherein the
15 first command within the sequence is assigned a MAC (message authentication code) with the aid of the random number and the secret key and all subsequent commands are assigned a MAC based on the MAC of the preceding command and the key.

17. Device including at least the following components:

a) Client at least including:

aa) a Browser

5 bb) a computer program product to execute unpacking of a data packet and transmission of individual commands thereof in sequence to a chipcard

cc) a reader for the chipcard

10 b) Server including at least:

aa) a computer program product to execute:

i) delivery of a secret code or Session Key by the server

15 ii) loading of a sequence of commands to download the application component to the chipcard

20 iii) generation of a digital signature with the secret key or Session Key by way of each command within the command sequence

iv) transmission of the signed
command sequence as a data packet to the
client

5

bb) a nonvolatile memory to store the
secret keys and the Master Key

c) Communication link between client and
server.

18. Client at least including:

a) a Browser

b) a computer program product to execute
unpacking of a data packet and transmission of
individual commands thereof in sequence to a chipcard.

5

19. Client in accordance with Claim 17 further including:

c) a chipcard reader

5 d) a chipcard with a nonvolatile memory at least containing the following data:

aa) a card number

bb) a card type

cc) a secret key

10

20. Computer program product stored in the internal memory of a digital computer, containing elements of software code to execute a method for downloading application components from a server via a client to a
5 chipcard, wherein the server and the client are interconnected via a distributed system, said method comprising:

a) delivery of a secret key or Session Key by the server;

10 b) loading of a sequence of commands to download the application component to the chipcard;

c) generation of a digital signature with the secret key or Session Key by way of each command within the command sequence;

15 d) transmission of the signed command sequence as a data packet to the client;

e) unpacking of the data packet and transmission of the individual commands in sequence to the chipcard; and

20 f) checking of the digital signature of the individual commands and execution of the commands if the digital signature is correct.

* * * * *

**SYSTEM AND METHOD FOR DOWNLOADING APPLICATION
COMPONENTS TO A CHIPCARD**

Abstract of the Disclosure

5 The present invention describes a method for
downloading application components, so-called on-card
application components, from a server via a client to a
chipcard, wherein the server and the client communicate with
each other via a distributed system, in particular an
10 Intranet or the Internet. The advantages of the present
invention lie in the fact that downloading of the
application components is divided into two stages: The first
stage occurs on the server only, and ensures that not every
command to download the application component is sent
15 individually over the network. This is effected by means of
a broadband-optimized protocol which bundles the individual
commands to download the application component into a
command sequence and sends it as a complete data packet over
the network. This reduces the time required for downloading
20 application components over the network. Each command within
the command sequence is assigned a digital signature and,
where appropriate, encrypted. This ensures that only
authenticated commands are accepted by the chipcard. In this
way this invention meets security requirements for the
25 transfer of data via distributed systems, in particular over
the Internet. The second stage occurs between the client
and the chipcard, and ensures that the data packets are
unpacked and sent individually to the chipcard. All
security-relevant keys and certificates are stored on the

secure server. Communication between the client and the server runs preferentially via SSL (Secure Sockets Layer) as the transfer protocol. Misuse of the inventive system/method is thereby rendered much more difficult.

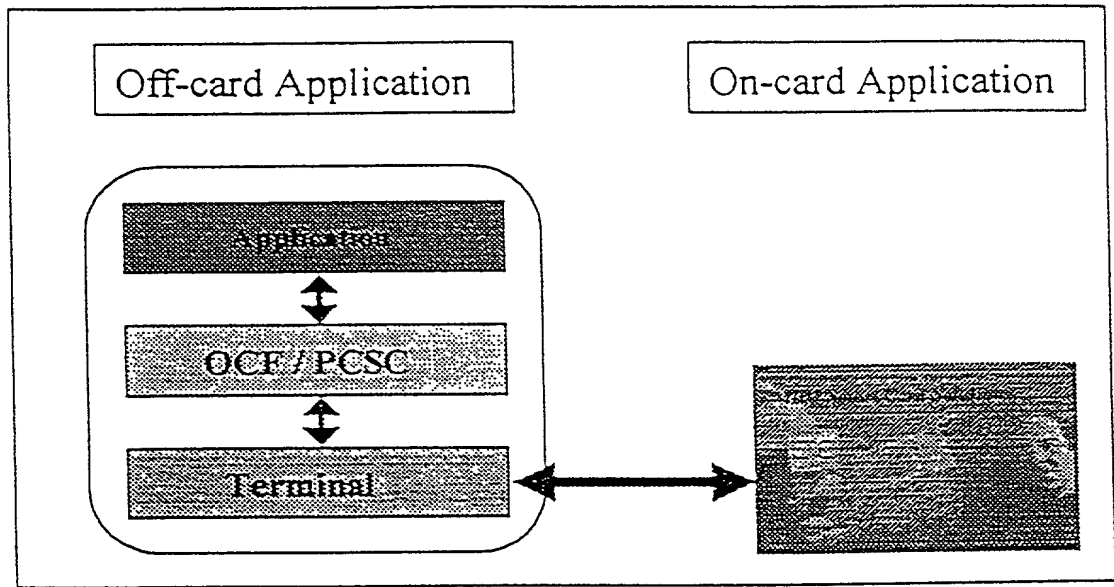


Fig. 1

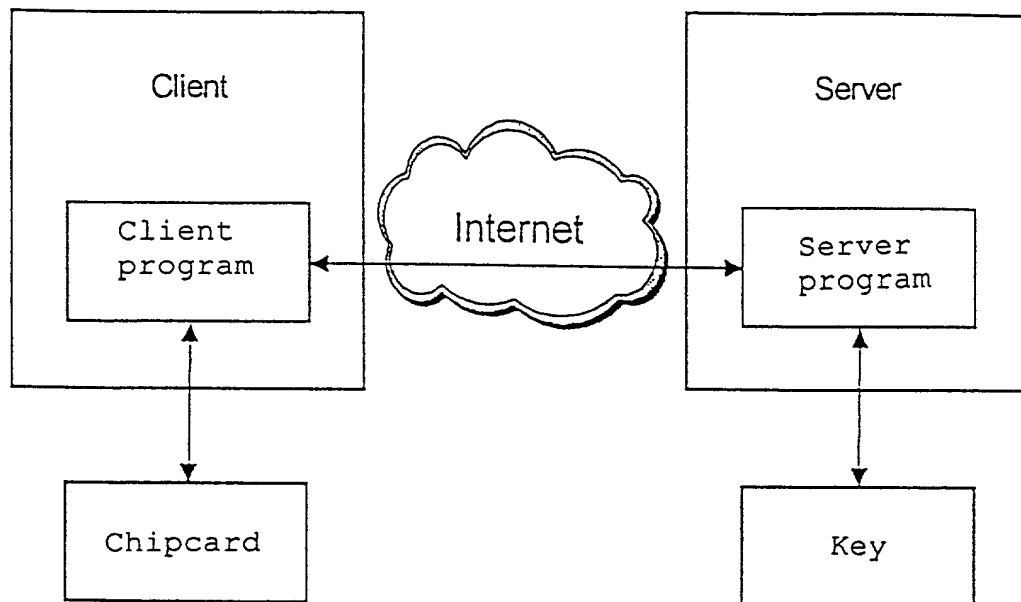


Fig. 2

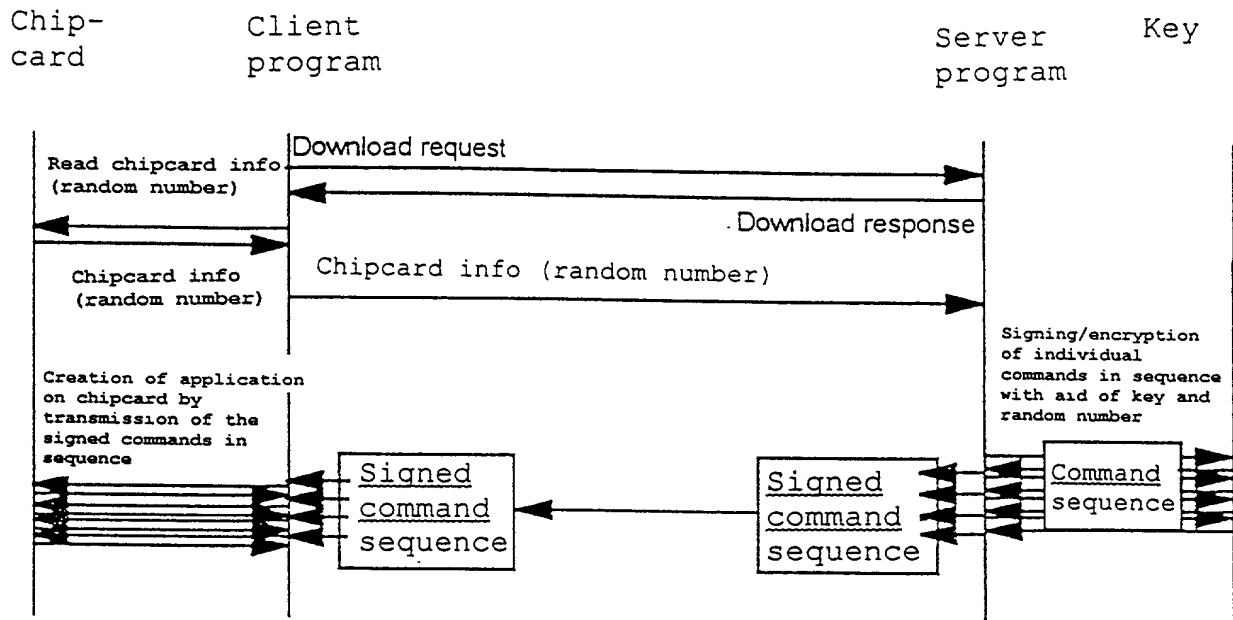


Fig. 3

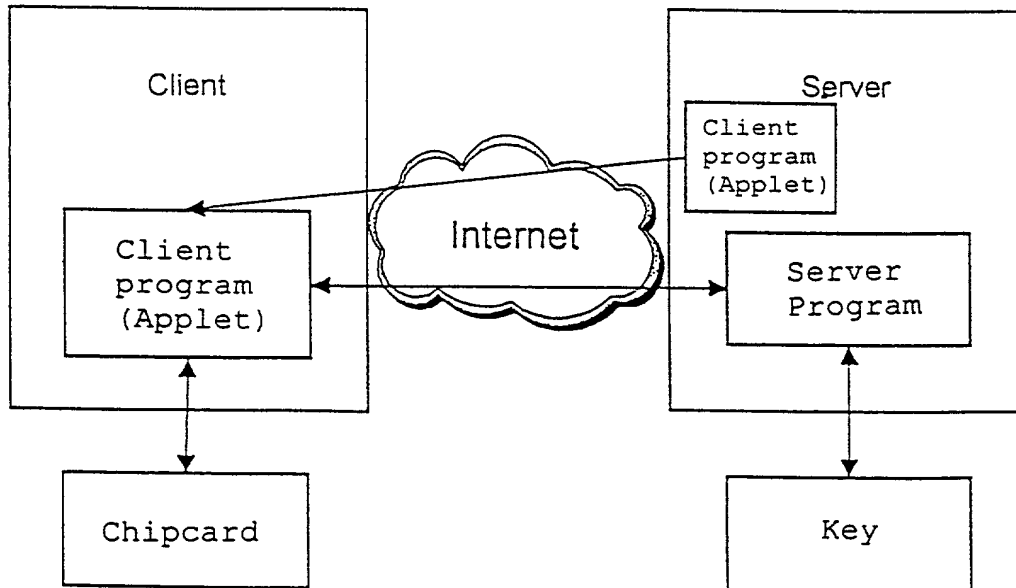


Fig. 4

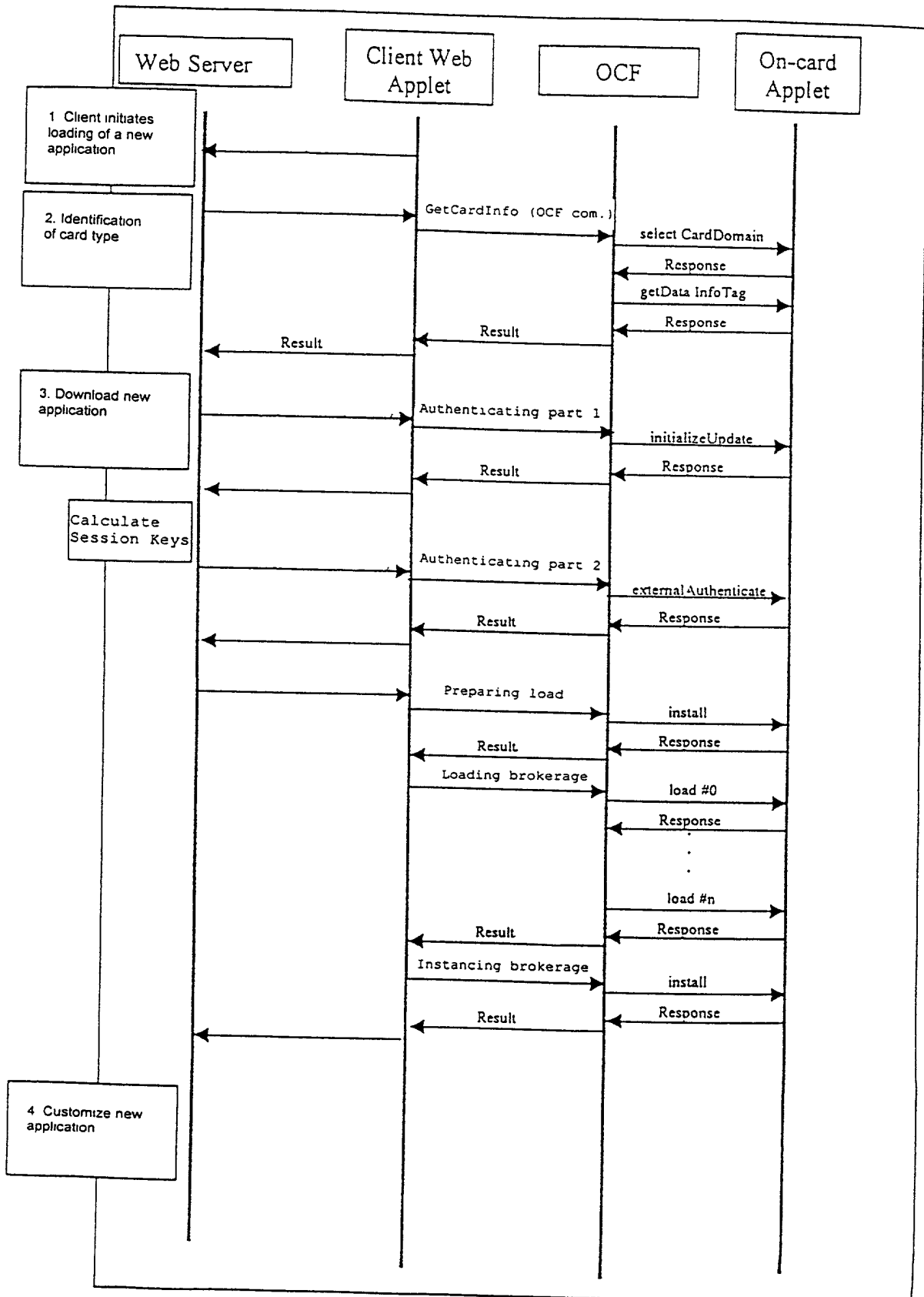


Fig. 5

Docket No.
DE919990073US1

Declaration and Power of Attorney For Patent Application

English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

SYSTEM AND METHOD FOR DOWNLOADING APPLICATION COMPONENTS TO A CHIPCARD

the specification of which

(check one)

☒ is attached hereto.

☐ was filed on _____ as United States Application No. or PCT International
Application Number _____
and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

Priority Not Claimed

199 47 986.0

Germany

5 October 1999

☐

(Number)

(Country)

(Day/Month/Year Filed)

☐

(Number)

(Country)

(Day/Month/Year Filed)

☐

(Number)

(Country)

(Day/Month/Year Filed)

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional application(s) listed below:

(Application Serial No.)

(Filing Date)

(Application Serial No.)

(Filing Date)

(Application Serial No.)

(Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

(Application Serial No.)

(Filing Date)

(Status)
(patented, pending, abandoned)

(Application Serial No.)

(Filing Date)

(Status)
(patented, pending, abandoned)

(Application Serial No.)

(Filing Date)

(Status)
(patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

Lynn L. Augspurger, Reg. No. 24,227

Lawrence D. Cutter, Reg. No. 28,501

Marc A. Ehrlich, Reg. No. 39, 966

William B. Porter, Reg. No. 33,135

Floyd A. Gonzalez, Reg. No. 26,732

William A. Kinnaman, Jr., Reg. No. 27,650

Lily Neff, Reg. No. 38,254

Andrew J. Wojnicki, Jr., Reg. No. 43,995

Christopher A. Hughes, Reg. No. 26,914

Edward A. Pennington, Reg. No. 32,588

John E. Hoel, Reg. No. 26,279

Joseph C. Redmond, Jr., Reg. No. 18,753

Jeff Rothenberg, Reg. No. 26,429

Kevin P. Radigan, Reg. No. 31,789

Blanche E. Schiller, Reg. No. 35,670

Send Correspondence to: **Kevin P. Radigan, Esq.**
HESLIN & ROTHENBERG, P.C.
5 Columbia Circle
Albany, NY 12203

Direct Telephone Calls to: *(name and telephone number)*
Kevin P. Radigan, Esq. (518) 452-5600

Full name of sole or first inventor STEFAN HEPPER	
Sole or first inventor's signature	Date
Residence Dorfackerstr. 22, D-72074 Tuebingen, Federal Republic of Germany	
Citizenship Germany	
Post Office Address Dorfackerstr. 22, D-72074 Tuebingen, Federal Republic of Germany	

Full name of second inventor, if any THOMAS SCHAECK	
Second inventor's signature	Date
Residence Am Muhrgraben 13, D-77855 Achern, Federal Republic of Germany	
Citizenship Germany	
Post Office Address Am Muhrgraben 13, D-77855 Achern, Federal Republic of Germany	